DISCUSSION DRAFT

Last revised on April 22, 2019

Buy Strong Internet of Things (IoT) Coalition White Paper

SUMMARY

- The U.S. Chamber of Commerce is exploring the creation of a Buy Strong Internet of Things (IoT) Coalition (the Coalition).[1] The group will advance smart public policies in this space and promote the production and deployment of secure IoT products internationally.

- The Chamber and the Coalition will convene discussions with multiple stakeholders to frame key problems and sell a solution(s) to a broader audience. The Coalition will shape the development and implementation of the core IoT cybersecurity capabilities baseline, which is being created by the National Institute of Standards and Technology (NIST) in partnership with the business community, including the CSDE C2.[2]

- A top Coalition priority will be for industry to achieve consensus on the technical criteria that underpin the IoT cyber baseline. The Coalition will leverage this core baseline to advocate for approaches to IoT device security that align with the interconnected nature of the global marketplace.

- The 2018 *Botnet Road Map* calls for establishing robust markets for consumer and industrial devices.[3] The Chamber wants the IoT ecosystem to benefit from businesses leading the development of cutting-edge devices and risk management activities. The Coalition will facilitate a process in the marketplace that generates both security and value for buyers and sellers.

The U.S. Chamber of Commerce is exploring the creation of a Buy Strong Internet of Things (IoT) Coalition (the Coalition) to promote the production, purchase, and deployment of more secure IoT products across the U.S. and abroad. The Chamber wants device makers, service providers, and buyers to gain from the business community leading the development of state-of-the-art IoT components and sound risk management practices. But which comes first—strong devices or strong market demand? Stakeholders are trying to think through and solve a chicken-and-egg strategy problem.

This initiative will leverage the IoT cybersecurity baseline that is being developed by the Department of Commerce, the private sector, and other stakeholders.[4] The Coalition will be composed of parties whose interests vary, yet are united toward a common goal: improving the security and resilience of the emerging IoT ecosystem.[5] The Chamber believes that the Coalition's activities are best summarized in four stages.

STATE THE PROBLEM(S)

First, the Coalition will need to frame the key problem(s) impacting the IoT cyber marketplace before jumping to possible solutions.[6] In speaking at length with stakeholders over the last two years, the Chamber has identified several challenges associated with IoT cybersecurity:

- **Security risk.** IoT objects are potentially vulnerable targets for hackers. As the number of IoT devices grows, so will the potential risk of successful intrusions and increases in costs from those incidents.[7] Strong IoT security should be a win-win proposition for makers, providers, and purchasers.[8]

- **Technical standards.** Industry and government share an interest in fostering stronger IoT security and resilience. The business community and the National Institute of Standards and Technology (NIST) are working diligently to deliver a core capabilities baseline for IoT devices that increases security, is dynamic in the face of threats, and is scalable internationally. A top Coalition priority will be for industry to achieve consensus on the technical criteria that support the IoT cyber baseline.

- **Public policy.** Some in government are pursuing policies that favor regulation and/or top-down certification schemes. The Chamber skeptical of policies that require specific approaches to security. Such mandates are unlikely to keep up with malicious actors or align with international best practices—outcomes that the Chamber presses the public and private sectors to pursue.[9]

- **Behavioral economics.** A number of IoT cyber advocates take a "build it and they will come" approach to IoT cyber, which tracks with traditional, rational notions of economics. Yet it is unclear if buyers—including individuals, households, businesses, and public institutions—will (1) be able to identify a strong device without a tool (not yet defined) to help them make educated choices[10] or (2) pay for the cost of additional security features.

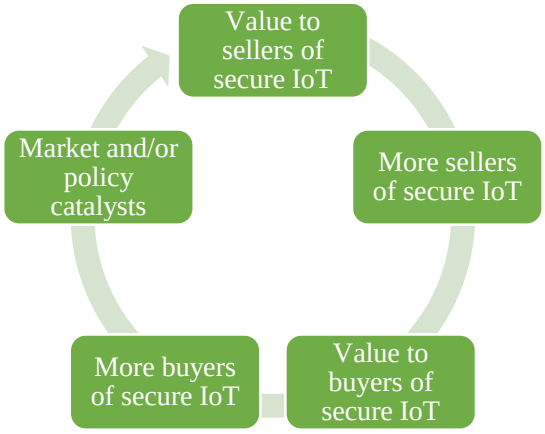
Most people's intuition is to buy the less expensive device even if the device's security is not strong—and possibly contrary to their own best interests. One function of the Coalition will be to better understand how people make real-world choices regarding purchasing IoT technology.[11]

The 2018 *Botnet Road Map* calls for establishing robust markets for consumer and industrial devices. The Chamber wants to get strong devices into the networks of businesses and the hands of consumers. Among other things, strong IoT will yield positive externalities. Of interest to policymakers, the social value of robust IoT will be greater than the private value.[12]

STRUCTURE AND ANALYZE CAUSES OF THE PROBLEM(S)

Second, once the Coalition has defined the problem(s)—particularly the role of buyer decision making—it will analyze the potential causes of this issue. The Chamber wants the IoT ecosystem to benefit from industry leading the development of cutting-edge devices and risk management activities. But which comes first—strong IoT objects or strong market signals? Stakeholders are wrestling with a classic chicken-and-egg problem.

The Coalition will explore facilitating a process in the marketplace that generates both security and value for buyers and sellers. Market and/or policy incentives may be needed to jump-start this circle.[13] The Coalition will advance the design, production, and demand for strong IoT devices in businesses, homes, and governments.



Worth flagging, decision-making research indicates that people tend to skip over the first two stages—stating and structuring problems—and jump right into finding the answers, which can be counterproductive. For example, brainstorming creates ideas for experimentation, but people tend not to grasp well the causes of the problem that they're attempting to solve.[14] The Chamber is planning to raise funds to conduct research. Getting specialists' insights into behavioral economics, marketing, and related subjects could add value to the Coalition's work.

Once the Coalition has evaluated the core factors that contribute to an apparent lack of demand for strong IoT devices, it will turn to generating and testing solutions.

GENERATE AND TEST SOLUTION(S)

Third, the Chamber recognizes that increasing IoT cybersecurity is a challenge that no allied group, much less a business association, can tackle alone. Any solution(s) that the Coalition develops needs to be ambitious yet manageable.[15] Proposed solutions also need to be tested to avoid mistakes. The Coalition should identify a target outcome that is specific and measureable. After it identifies a range of possible solutions, it should focus on one or two. The Coalition could introduce the change in some area of the market (the treatment group) and not in others (the control group).[16]

SELL THE SOLUTION(S)

Fourth, the last problem-solving stage features selling. It is difficult for a coalition that that comes up with a solution(s) to also have the influence and resources to implement it alone. This means that the Coalition is going to have to persuade other people to buy into its goals and want to help.

COALITION STRUCTURE AND QUESTIONS TO ANSWER

The Chamber is identifying groups that could participate in and provide resources to the Coalition, which will be as inclusive as possible. It will be open to Chamber members, of course, and draw on the shared interests and expertise of allies, opponents, and fence sitters.[17] Equally important, Coalition members and the Chamber need to consider the following:

- **Agenda.** Is it clearly defined? Will Coalition members be willing to change their minds as they uncover new information?

- **Support.** How will the Coalition determine which players are most important?

- **Focus.** Whom will the Coalition go to first? How will it sequence subsequent efforts?

- **Players.** How will the Coalition deal with competing factions? How will it manage competing agendas?[18]

Endnotes

---

[1] The Buy Strong Internet of Things (IoT) Coalition is a working title.

[2] At the time of this writing, the Council to Secure the Digital Economy (CSDE) and the Consumer Technology Association (CTA) are coordinating the development of an industry-led consensus—which its participants call the CSDE C2 (short for "convening the conveners")—regarding cybersecurity capabilities that would be common to new IoT devices.

[3] The Department of Commerce and the Department of Homeland Security (DHS), *Road Map: Building a More Resilient Internet* (aka the *Botnet Road Map*), November 29, 2018. https://www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet

[4] Katerina Megas, "Let's talk about IoT device security," the National Institute of Standards and Technology (NIST), February 4, 2019.
https://www.nist.gov/blogs/i-think-therefore-iam/lets-talk-about-iot-device-security
https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

On February 7, 2019, 24 associations sent a letter to the White House to urge the administration and Congress to support NIST's efforts alongside industry to bolster IoT security.
https://www.uschamber.com/sites/default/files/2-7-19_multi-association_wh_letter_iot_cybersecurity_final.pdf

[5] Herminia Ibarra and Jennifer M. Suesse, *Building Coalitions*, Harvard Business School case study, revised April 9, 1997.

[6] Readers of this paper are encouraged to listen to "The Right Way to Solve Complex Business Problems," Harvard Business Review (HBR) IdeaCast, December 4, 2018.
https://hbr.org/ideacast/2018/12/the-right-way-to-solve-complex-business-problems

[7] Eric A. Fischer, *The Internet of Things: Frequently Asked Questions*, Congressional Research Service (CRS), October 13, 2015, pg. 14.
https://fas.org/sgp/crs/misc/R44227.pdf

[8] Some 50 billion devices will be connected to the internet by 2020. According to the U.S. Chamber of Commerce's estimates, the IoT could add roughly $15 trillion to global GDP over the next 20 years. See the Chamber's testimony before the House Oversight and Government Reform Committee Information Technology Subcommittee hearing, "Cybersecurity of the Internet of Things," October 3, 2017.
https://www.uschamber.com/sites/default/files/10-3-17_testimony_iotcybersecurity_house_ogr_final.pdf

[9] The Chamber would welcome clear steps by government officials to elevate their defense of industry and the IoT ecosystem.

[10] John Beshears and Francesco Gina, "Leaders as Decision Architects," HBR, May 2015. According to this article, all employees commit preventable mistakes (e.g., underestimating how long it will take to finish a project or focusing too much on information that supports their current views). It is difficult to rewire the human brain to undo the patterns that lead to such mistakes. But there is another approach: alter the environment in ways that encourage people to make decisions that lead to good outcomes. Such thinking—aka choice architecture—could be applied to how people acquire IoT devices.
https://hbr.org/2015/05/leaders-as-decision-architects

[11] Richard H. Thaler, *Misbehaving: The Making of Behavioral Economics* (W.W. Norton and Company: New York, 2015).

[12] On positive externalities, see N. Gregory Mankiw, *Principles of Economics, Third Edition* (Thomson: U.S., 2004), pg. 207.

[13] Chamber letter to NIST on NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (NISTIR), October 24, 2018. The graphic was inspired, in part, by the Strategic Toolkits webpage, "Chicken and Egg Strategy Problems."
http://strategictoolkits.com/strategic-concepts/chicken-and-egg-strategy-problems

https://www.uschamber.com/sites/default/files/10-24-18_u.s._chamber_comment_letter_draft_nistir_8228_final.pdf

[14] Ed O'Brien, "We Use Less Information to Make Decisions Than We Think," HBR, March 7, 2019. https://hbr.org/2019/03/we-use-less-information-to-make-decisions-than-we-think

Nadav Klein and Ed O'Brien, "People use less information than they think to make up their minds," *Proceedings of the National Academy of Sciences* (PNAS), December 10, 2018. https://www.pnas.org/content/115/52/13222 https://www.pnas.org/content/pnas/115/52/13222.full.pdf

[15] Amitava Chattopadhyay, Antonios Stamatogiannakis, and Dipankar Chakravarti, "Why You Should Stop Setting Easy Goals," HBR, November 27, 2018. This article is relevant to the Coalition. It notes that when setting team goals, many managers feel that they must maintain a tricky balance between setting targets high enough to achieve impressive results and setting them low enough to keep the troops happy.

But the assumption that employees are more likely to welcome lower goals doesn't stand up to scrutiny. In fact, research indicates that *in some situations people perceive higher goals as easier to attain* than lower ones—and even when that's not the case, they still can find those more challenging goals more appealing. https://hbr.org/2018/11/why-you-should-stop-setting-easy-goals

[16] "Leaders as Decision Architects" (2015).

[17] The authors of *Building Coalitions* define several groups that typically compose a coalition's political landscape, which are adapted here for the Buy Strong IoT Coalition:

- Allies. This group refers to people who agree with and trust the Coalition's goals. Allies are the core members of the Coalition.

- Opponents. These people are not the same as adversaries (who are untrustworthy and oppose the Coalition's agenda), as one may assume. Opponents share high trust but low agreement with the Coalition's objectives. The task of opponents is to bring out the best in the Coalition by challenging it.

- Fence sitters. Fence sitters gather data from the Coalition and usually make their own informed decisions. They probably won't help or hurt the Coalition much.

[18] *Building Coalitions* (1997), pg. 7.